

**Improvements Made But Actions Still Needed
to Prevent Computer Virus Infections**

June 2002

Reference Number: 2002-20-117

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
For TAX
ADMINISTRATION

June 27, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Scott E. Wilson

FROM: (for) Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Made But Actions Still
Needed to Prevent Computer Virus Infections
(Audit # 200120020)

This report presents the results of our review of the controls in place to prevent and detect computer viruses. The overall objective of this review was to determine whether the Internal Revenue Service (IRS) is adequately preventing and detecting computer viruses. This review is a follow-up to our previous report titled, *A Comprehensive Program for Preventing and Detecting Computer Viruses Is Needed* (Report Reference Number 2000-20-094, dated June 2000).

In summary, we found that since our previous report, the virus protection program at the IRS has received increased attention and has matured to the point where responses to virus attacks have been significantly more effective. Although the IRS has experienced a number of virus attacks since our last review, only one of the attacks has caused significant damage to computer systems. The IRS estimated its direct recovery costs at \$950,000, for this incident, in addition to the approximately \$600,000 of computer downtime. While costly, the IRS was able to limit its exposure to other viruses and consequently spent \$10 million less than other similarly sized organizations have had to spend in the past.

We attribute much of this success to progress made in installing anti-virus software on employees' workstations as we recommended in our prior report. Ninety-seven percent of the workstations we tested in this review had the latest version of anti-virus software. Early detection efforts have also improved and decisions to shut down and isolate viruses are made faster.

The IRS cannot rely solely on anti-virus software to prevent and detect viruses, however. Because of the delay between the time that a virus is created and the time

anti-virus vendors develop a detection solution, new viruses have a potential to pass undetected into the IRS computer network. Also, access to the Internet has greatly increased the risk of introducing viruses. While the IRS' email firewalls effectively monitor and detect viruses sent to IRS employees' official email addresses, the IRS does not scan viruses at its Internet gateways leaving it vulnerable to viruses introduced through employees' personal email accounts over the Internet. During our audit period, a significant number of accesses were made to these personal email accounts from IRS computers. These accesses bypassed the IRS email firewalls.

The IRS is also vulnerable to viruses from certain Internet web sites. Many web sites contain embedded computer scripts that expose applications and files on employees' workstations to viruses. These scripts are invisible to the employees. Most of the IRS workstations we tested did not warn employees when they accessed a web site containing these scripts.

To address these risks, we recommend that the IRS block employee access to all non-IRS email providers; reinforce the IRS policy that employees not be allowed to access personal email accounts from IRS computers; and block or warn employees when they attempt to access an Internet site that uses certain scripts that could contain viruses.

Management's Response: Management agreed with the recommendations presented in this report, and corrective actions have been taken to address the risks identified. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have any questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background	Page 1
The Internal Revenue Service Has Improved Its Virus Detection Efforts...	Page 2
More Can Be Done to Prevent the Introduction of Viruses	Page 2
<u>Recommendations 1 through 3:</u>	Page 5
Appendix I – Detailed Objective, Scope, and Methodology	Page 7
Appendix II – Major Contributors to This Report.....	Page 8
Appendix III – Report Distribution List	Page 9
Appendix IV – Management’s Response to the Draft Report	Page 10

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

Background

Computer viruses are unauthorized computer programs designed to spread without detection across computer systems and networks. McAfee, a leading vendor of anti-virus software, reported that as of March 2002, there were more than 57,000 viruses in existence, with new viruses being developed every day. Along with this growth has been the creation of more complex viruses that are increasingly difficult to detect.

Some viruses are capable of causing computer system crashes, corruption of computer files, unauthorized disclosure of information, and destruction of data. This kind of damage could be particularly critical to organizations such as the Internal Revenue Service (IRS) due to the sensitivity of the taxpayer data handled by the agency. The cost of responding to virus infections and the negative impact on productivity caused by computer downtime can also be significant.

The IRS has been exposed to a number of viruses over the past several years. According to the ICSA.net, an Internet security assurance services firm, organizations the size of the IRS spend up to \$11.5 million annually to recover from virus incidents. The ICSA.net also reported that viruses cost United States companies over \$2 billion in 1999, and that the Melissa virus alone cost North American businesses an estimated \$93 million to \$385 million in actual damages during the one week following its release. The Melissa virus infected more than one million personal computers.

To determine whether the IRS is adequately preventing and detecting computer viruses, we tested a judgmental sample of 149 IRS computers located in New Carrollton, Maryland (50 computers), Milwaukee, Wisconsin (50 computers) and Boston, Massachusetts (49 computers). Our fieldwork was conducted between September and December 2001.

The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

The Internal Revenue Service Has Improved Its Virus Detection Efforts

Since our previous report titled, *A Comprehensive Program for Preventing and Detecting Computer Viruses Is Needed* (Report Reference Number 2000-20-094, dated June 2000), the IRS has experienced only one significant virus attack. The IRS estimated its direct recovery costs at \$950,000, for this incident, in addition to the approximately \$600,000 of computer downtime. While costly, the IRS was able to limit its exposure to other viruses and consequently spent \$10 million less than other similarly sized organizations have had to spend in the past.

We attribute this success to progress made in detecting viruses. In response to a recommendation in our prior report, the IRS properly assigned responsibility for the anti-virus program to the Deputy Director-Computer Security for Incident Response. His actions to install anti-virus software on workstations have significantly improved the IRS' ability to detect virus infections. Every workstation we tested in this review had anti-virus software installed, and 97 percent of those had the latest version of anti-virus software. When we conducted our prior review, no single manager was responsible for the virus program and anti-virus software was either not installed or out of date.

The IRS has also established an early detection process to identify, review and delete email attachments that could contain viruses. When viruses are detected, security specialists are alerted and actions are taken to prevent the spread of the virus.

More Can Be Done to Prevent the Introduction of Viruses

Anti-virus software should detect and destroy any virus that has been identified by the software vendor. It is still possible, however, that a damaging virus could infect the IRS before the software vendor identifies and provides the solution. For that reason, the IRS needs to ensure that suspicious files are prevented from entering the IRS network.

Viruses can still be introduced by accessing personal email

A Computer Virus Prevalence Survey, conducted in 2000 by the ICSA Labs, showed that approximately 87 percent of reported virus attacks came by way of email attachments.

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

These viruses usually contain code to automatically send the virus to email addresses maintained on the infected computer. Thus, they can spread very quickly and alter, damage or delete files.

The IRS has improved its virus protection by preventing various file attachments that could contain computer viruses from being transmitted from one employee to another. The email system is configured to block all files with certain pre-designated extensions. In these cases, the sender is informed by a return email that the attachment has been deleted because an unauthorized file was found.

Emails sent from non-employees to an IRS employee's official email address must go through an email server. The IRS email servers prevent certain files that could contain viruses from being forwarded to the IRS employees' official email addresses.

However, employees can still introduce viruses into the IRS network by accessing personal email accounts via Internet browsers at sites such as Yahoo, AOL and Hotmail. In September 2001, the IRS was infected by the NIMDA¹ virus in this very way. Employees using Internet browsers to obtain email circumvent the controls used by the IRS' email servers. The IRS has to rely on employees to use virus detection software on their workstations in these situations.

To determine the extent of employee usage of external email, we obtained firewall audit logs from the primary Internet gateway, for the period November 1 to 7, 2001. Based on an analysis of these logs, we estimate that about 1,700 employees used email via the Internet gateway each workday.

IRS policy prohibits employees' access to personal email accounts. However, the IRS has done little to enforce this policy. Controls were not put in place at the IRS Internet gateway to prevent these accesses. The IRS was aware of the risks associated with personal email accounts but had not taken corrective actions due to other priorities.

¹ The NIMDA computer worm/virus spreads itself through email and other methods to create an opening on infected computers, allowing potential unauthorized access.

Viruses can still be introduced by accessing web pages

A newly emerging security threat comes from small applications known as Malicious Mobile Code (MMC). Employees can unknowingly download MMCs just by accessing an Internet web site possibly causing computers or files to become corrupted.

ActiveX controls,² present in some web pages, represent significant security risks for computer users accessing the Internet because:

- Unauthorized individuals (hackers) could surreptitiously use ActiveX controls embedded in a web page to gain access to the Internet user's computer.
- ActiveX controls embedded in a web page are potential entry points for computer viruses or MMCs.

Of the 149 IRS computer workstations we examined, 27 did not provide the capability for employees to exchange information with these web sites. Of the remaining 122 workstations, only 2 warned employees about ActiveX controls embedded in the web sites accessed from their workstations.

The IRS has recognized the risk of these applications and is now blocking the execution of ActiveX controls on newly deployed workstations. This is being accomplished with the implementation of the Common Operating Environment (COE) throughout the IRS. The IRS "COE System Policies" state that there is an inherent risk associated with downloading and running ActiveX controls from the Internet. The workstations included in this environment will contain standard settings that will block employees' from accessing these ActiveX web sites.

² ActiveX controls contain computer code designed to work through Internet Explorer browsers, versions 3.0 or higher. The interactive components of these controls expose the applications and files contained on workstations to viruses. ActiveX controls are invisible to the casual Internet user.

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

Some employees may need to access ActiveX web sites for business reasons. The IRS has agreed to allow access to these employees but had not considered the need to warn them of the security risks.

Recommendations:

We recommend that the Deputy Commissioner for Modernization & Chief Information Officer:

1. Configure firewalls at all Internet gateways to prevent employees from accessing personal email accounts.
2. Re-emphasize the policy that employees are not allowed to access personal email accounts from IRS computers. Consider implementing penalty provisions for noncompliance.
3. Continue efforts to block employees' access to ActiveX web sites unless they have a business need to access these sites. For those employees with a business need, configure firewalls at all Internet gateways to display a warning on their workstations that the site could contain viruses. The warning should give employees the option of continuing to review the site if they are confident that viruses do not exist.

Management's Response: The IRS installed Surf Control software, which blocks all web-based email. This was done to prevent users from accessing inappropriate web sites as defined by IRS policy. Management issued a "Limited Personal Use of Government Information Technology Equipment/Resources" policy that reiterates the prohibition on accessing personal email accounts. The policy addresses sanctions/penalties for misuse. The use or non-use of ActiveX controls will be controlled at the workstation and not at the firewall. Use of ActiveX controls outside the firewall will be limited to those users who can demonstrate a clear business need and will require an approval by the Deputy Commissioner for Modernization & Chief Information Officer as well as an exception granted by the Department of the Treasury's Office of Security. When ActiveX is in use, the customer will be prompted or warned

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

that the site could contain viruses, and given the option of continuing the operation.

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) is adequately preventing and detecting computer viruses. This review is a follow-up to our previous report entitled, *A Comprehensive Program for Preventing and Detecting Computer Viruses Is Needed* (Report Reference Number 2002-20-094, dated June 2000).

- I. To evaluate the effectiveness of the policies, procedures, methods, and data used by IRS management to oversee the virus protection program, keep virus protection current, and prevent the introduction and spread of viruses, we:
 - A. Determined whether the Deputy Commissioner for Modernization & Chief Information Officer formally assigned the responsibility for directing and overseeing the implementation and effectiveness of the IRS' virus prevention efforts to a senior official. We interviewed the appropriate management official and reviewed any relevant documentation maintained by the management official.
 - B. Determined whether the official responsible for the virus program had developed and implemented IRS-wide procedures detailing the frequency and steps to be followed for reliably updating anti-virus software on both desktop and portable computers.
 - C. Determined whether the official responsible for the virus program had established controls to ensure that all anti-virus updates have been successfully completed.
- II. To determine whether the IRS is adequately preventing and detecting computer viruses, we:
 - A. Tested a judgmental sample of 149 IRS computers located in New Carrollton, Maryland (50 computers), Milwaukee, Wisconsin (50 computers), and Boston, Massachusetts (49 computers). We randomly selected these computers from various functions within each location. An Information Services employee accompanied us during our testing, although the selection for testing was done by an auditor.
 - B. Determined whether outside (non-IRS) email is filtered by the Department of the Treasury and the IRS firewalls and gateways. Specifically, we attempted to access and use an outside email provider via an IRS Internet connection. We analyzed firewall logs for the period November 1 to 7, 2001, at the primary Internet gateway to determine how frequently IRS employees access personal email accounts.
 - C. Determined whether ActiveX script controls uniformly exist across the IRS networks, and what those controls were.

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Gerald Horn, Audit Manager
Dan Ardeleano, Senior Auditor
Charles Ekholm, Auditor
William Simmons, Auditor

Report Distribution List

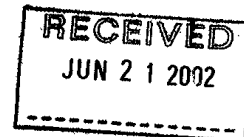
Commissioner N:C
Deputy Commissioner N:DC
Director, Tax Administration Coordination N:ADC:T
Director, Office of Security M:S
Chief, Information Technology Services M:I
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaison: Deputy Commissioner for Modernization & Chief Information Officer M

Management's Response to the Draft Report



DEPUTY COMMISSIONER


DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



June 20, 2002

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:


John C. Reece
Deputy Commissioner for Modernization &
Chief Information Officer

SUBJECT:

Response to Draft Report – Improvements Made But Actions Still
Needed To Prevent Computer Virus Infections (Audit #
200120020)

We have reviewed your draft report and recommendations about preventing and detecting computer viruses. We have made progress in this area, and we assigned the anti-virus program to the Deputy Director, Computer Security for Incident Response, as you recommended in your prior report.

In this draft report, you identified our potential vulnerabilities to viruses. We have completed corrective actions on two of the three report recommendations. We will complete corrective actions for the remaining recommendation by the end of this month. Our management goal is to continually strive for an enhanced security program that effectively manages risks. Therefore, we appreciate your comments; they will assist us in strengthening our efforts to prevent and detect viruses. Enclosed is a detailed response to each of your report recommendations.

If you have any questions or concerns, please contact me at (202) 622-6800, or Mr. Len Baptiste, who directs the IRS security program, at (202) 622-8910.

Enclosure

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

Management response to Draft Audit Report – Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

RECOMMENDATION #1:

Configure firewalls at all Internet gateways to prevent employees from accessing personal e-mail accounts.

ASSESSMENT OF CAUSE:

Even though IRS policy prohibited the access of private e-mail accounts using the Internet, no automated method existed to prevent such accesses.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The IRS identified and installed Surf Control software to prevent users from accessing inappropriate web sites as defined by IRS policy. This software blocks all web-based e-mail. In addition, on May 13, 2002, the IRS issued a "Limited Personal Use of Government Information Technology Equipment/Resources" policy that reiterated the prohibition on accessing personal e-mail accounts using the Internet. This policy also allowed employees to use their government e-mail account for personal communication, in part to mitigate the employees' need to access personal e-mail accounts.

IMPLEMENTATION DATE:

Completed, February 19, 2002

Policy reinforced and became effective May 13, 2002

RESPONSIBLE OFFICIAL:

Director, Mission Assurance

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

RECOMMENDATION #2:

Re-emphasize the policy that employees are not allowed to access personal e-mail accounts from IRS computers. Consider implementing penalty provisions for noncompliance.

ASSESSMENT OF CAUSE:

We had not recently publicized our long-standing policy prohibiting access to personal e-mail accounts from IRS computers and enforcement efforts were minimal.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We developed and implemented a new Limited Personal Use policy for Internet, e-mail, and other equipment and resources that became effective May 13, 2002. The policy clearly delineates inappropriate personal use including access to private e-mail accounts through the Internet. We highlighted this policy in the IRS Headlines newsletter dated May 13, 2002, which has agency-wide distribution. In addition, the policy addresses sanctions/penalties for misuse.

We will continue to ensure that the executives, managers, and employees are aware of this policy through periodic awareness forums.

IMPLEMENTATION DATE:

Completed, May 13, 2002

IRS policy on "Limited Personal Use of Government Information Technology Equipment Resources" became effective May 13, 2002.

RESPONSIBLE OFFICIAL:

Director, Mission Assurance

Improvements Made But Actions Still Needed to Prevent Computer Virus Infections

RECOMMENDATION #3:

Continue efforts to block employees' access to Active X web sites unless they have a business need to access these sites. For those employees with a business need, configure firewalls at all Internet gateways to display a warning on their workstations that the site could contain viruses. The warning should give employees the option of continuing to review the site if they are confident that viruses do not exist.

ASSESSMENT OF CAUSE:

During the course of the audit, we were in the process of blocking the execution of Active X controls.

CORRECTIVE ACTION TO RECOMMENDATION #3:

By the end of June 2002, the use, non-use and warning of use of Active X controls will be appropriately controlled at the workstation level and not at the firewall. These controls will include having browser settings for the corporate standard workstation configuration to allow unrestricted use of Active X controls inside the firewall. Use of Active X controls outside the firewall will be limited to only those users who can demonstrate a clear business need. A customer's use of Active X controls outside the firewall will require an approval by our CIO, as well as an exception that must be granted by Treasury's Office of Security. When Active X is in use, the customer will be prompted or warned that the site could contain viruses, and given the option to continue or abort the operation.

IMPLEMENTATION DATE:

July 1, 2002

RESPONSIBLE OFFICIAL:

Director, End User Equipment Services